Report on Compliance with Laws and Regulations

ERNST & YOUNG

Ernst & Young LLP
1225 Connecticut Avenue, N.W.
Washington, DC 20036

Phone: (202) 327-6000
Fax: (202) 327-6200
www.ey.com

Report on Compliance with Laws and Regulations

To the Inspector General
U.S. Department of Education

We have audited the consolidated balance sheet of Federal Student Aid (FSA), a performance-based organization of the U.S. Department of Education (the Department) as of September 30, 2006, and the related consolidated statements of net cost, changes in net position, and financing and the combined statement of budgetary resources for the fiscal year then ended, and have issued our report thereon dated November 7, 2006. We conducted our audit in accordance with auditing standards generally accepted in the United States; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 06-03, *Audit Requirements for Federal Financial Statements*.

The management of FSA is responsible for complying with laws and regulations applicable to the entity. As part of obtaining reasonable assurance about whether the entity's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts and certain other laws and regulations specified in OMB Bulletin No. 06-03, including the requirements referred to in the Federal Financial Management Improvement Act of 1996 (FFMIA). We limited our tests of compliance to these provisions, and we did not test compliance with all laws and regulations applicable to FSA.

The results of our tests of compliance with the laws and regulations described in the preceding paragraph exclusive of FFMIA disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 06-03. We noted certain other matters involving compliance with laws and regulations that were reported to management in a separate letter dated November 7, 2006.

Under FFMIA, we are required to report whether FSA's financial management systems substantially comply with the Federal financial management systems requirements, applicable Federal accounting standards, and the U.S. Standard General Ledger at the transaction level. To meet this reporting requirement, we performed tests of compliance with FFMIA section 803(a) requirements.

The results of our tests disclosed instances in which the Department's financial management systems did not substantially comply with certain requirements discussed in the preceding paragraph. FSA relies on the Department's systems to provide support for FSA's financial reporting needs, including utilizing the Department's general ledger to process transactions. We have identified the following instance of noncompliance:

ERNST & YOUNG

Ernst & Young LLP

While the Department and FSA have made progress in strengthening controls over information technology processes and have continued making improvements in the areas of configuration management, virus protection, and security patch management during FY 2006, our audit work and audit reports prepared by the Office of Inspector General (OIG) identify certain control weaknesses, including several that were repeat conditions, within information technology security and systems that need to be addressed. More specifically, the Department and FSA should: (1) strengthen access controls to protect mission critical systems (e.g. user provisioning process, periodic access revalidation, timely removal of user access, physical data center access controls); (2) improve the configuration management process to ensure consistent security configuration of servers and mainframe security packages across the organization and improve configuration settings to comply with best practices; (3) enforce the use of complex passwords in all systems across the organization; (4) comprehensively review technical security weaknesses identified in prior audits in order to determine whether security controls have been fully implemented or adequately address the security weaknesses across the organization; (5) implement consistent tape back up controls; (6) strengthen security incident handling procedures and intrusion detection systems; (7) consistently perform risk assessments and Certification and Accreditation on its new systems and new environments, especially after migrating to a new location or a new system; (8) improve private data protection controls (e.g. proper disclosure of the use of 'cookies' on Department and FSA websites and polices and procedures on dial up access and encryption of back up data); (9) enhance its security training and awareness program and the monitoring of this program, specifically in accounting for completion of such training by all employees and contractors; (10) improve protection of sensitive information, including read-only access to personally identifiable information on Department and FSA systems; and (11) the Office of Management should continue its efforts to reconstruct its inventory database or otherwise reconcile its physical inventory of computing and other equipment to ensure that all Department and FSA computing resources and the data residing in them are secured and safeguarded.

The Report on Internal Control includes additional information related to the financial management systems that were found not to comply with the requirements of FFMIA relating to information technology security and controls. It also provides information on the responsible parties, relevant facts pertaining to the noncompliance with FFMIA, and our recommendations related to the specific issues. We have reviewed our findings and recommendations with management of the Department and FSA. Management concurs with our recommendations and, to the extent findings and recommendations were noted in prior years, has provided a proposed action plan to the OIG in accordance with applicable Department directives.

Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit and, accordingly, we do not express such an opinion.

ERNST & YOUNG

Ernst & Young LLP

This report is intended solely for the information and use of the management of FSA and the Department, OMB, Congress, and the Department's OIG, and is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

November 7, 2006